

REMARKS

The present application was filed on September 12, 1997 with claims 1-26. The Examiner rejected claims 1-26 under 35 U.S.C. §103 as being unpatentable over U.S. Patent No. 5,606,668 to Shwed. After responses traversing the rejection, Applicants appealed the rejections. In an Appeal Decision dated January 14, 2004, the Board of Patent Appeals and Interferences upheld the rejections.

In view of the Appeal Decision, Applicants filed a Request for Continued Prosecution along with an amendment that amended independent claims 1, 8, 12, 16, 17 and 22. Such an amendment was made in an effort to further clarify the subject matter of the invention and expedite the case through to issuance.

In the present Office Action, the Examiner has: (i) rejected claims 3-5 under 35 U.S.C. §112, second paragraph, as being indefinite; (ii) rejected claims 1-26 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,835,726 to Shwed et al. (hereinafter Shwed '726); and (iii) rejected claims 1-26 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,606,668 to Shwed (hereinafter Shwed '668).

In this response, Applicants: (i) amend claims 3 and 4 to address the §112, second paragraph, rejection; and (ii) respectfully traverse the various §102(e) and §103(a) rejections for at least the following reasons.

Regarding the §112, second paragraph, rejection of claims 3-5, Applicants have amended claims 3 and 4 to address the lack of antecedent basis with respect to the word "set." Accordingly, withdrawal of the §112, second paragraph, rejection is respectfully requested.

Regarding the §102(e) and §103(a) rejections of claims 1-26, since both Shwed '726 (subject of the §102(e) rejection) and Shwed '668 (subject of the §103(a) rejection) fail to teach or suggest all limitations of the claimed invention, Applicants will address the two grounds of rejection jointly below.

As mentioned above, Applicants previously amended independent claims 1, 8, 12, 16, 17 and 22. More particularly, claims 1, 8, 12, 17 and 22 were amended to recite that a security policy comprises multiple rules. Independent claim 16 was amended to recite that a domain comprises at

least one security policy and a security policy comprises multiple rules, and that a plurality of administrators are associated with the plurality of domains.

Applicants amended the claimed invention to further make clear the distinction between a security policy and a rule. That is, a security policy comprises multiple rules. Thus, by way of example, independent claim 1 recites a method for validating a packet in a computer network, comprising the steps of: deriving a session key for said packet; selecting at least one of a plurality of security policies as a function of the session key, wherein a security policy comprises multiple rules; and using the selected at least one of the security policies in validating said packet.

Thus, as is clearly recited, when a packet is received, for example, by a computer implementing the methodology, first a security policy is selected from among a plurality of security policies, then the security policy comprised of its multiple rules is used to validate the packet. Thus, the invention effectively provides a hierarchical rule selection procedure. That is, before a rule is applied to a particular packet, the appropriate security policy is first selected and then, a rule from the selected security policy is applied to the packet.

Neither Shwed '726 nor Shwed '668 teach or suggest selecting a security policy having multiple rules from among a plurality of security policies, each having multiple rules.

FIG. 3 of both Shwed references have been cited in support of the rejection. As column 4, lines 49-50, of Shwed '726 states "FIG. 3 shows the computer screen of the network administrator." Then, column 6, line 62, through column 7, line 11, of Shwed '726 go on to explain:

FIG. 3 shows the computer screen 206 in FIG. 2 in more detail. The screen is broken into four windows, two smaller windows at the left side and two larger windows at the right side. Network objects and services are two aspects of the network which must be defined in the security method of the present invention. Window 304 is used to define network objects such as the workstations, gateways and other computer hardware connected to the system. It is also possible to group various devices together such as, for example, the finance department, the research and development department, the directors of the company. It is thus possible to control data flow not only to individual computers on the network, but also to groups of computers on the network by the appropriate placement of packet filters. This allows the system operator have a great deal of flexibility in the managing of communications on the network. It is possible for example to have the chief financial officer as well as other higher ranking officials of the company such as the CEO and the directors able to communicate directly with the finance group, but filter out communications from

other groups. It is also possible to allow electronic mail from all groups but to limit other requests for information to a specified set of computers. This allows the system operator to provide internal as well as external security for the network. The object definition would include the address of the object on the network, as well as a name or group whether the object is internal or external to the network, whether or not a packet filter has been installed on this object and a graphical symbol. The graphical symbol is used in connection with the rule base manager 302.

However, this portion of Shwed '726 merely refers to the fact that a network administrator may specify different security rule sets for different business entities. However, as clearly explained at column 6, lines 42-45, a rule set specified by the network administrator is then processed by the packet filter generator 208 and the resulting code is transmitted to the appropriate packet filter in the network to perform the function that is desired. Then, as explained at column 9, lines 18-50, a packet entering the computer, at a particular connection, on which the packet filter resides is diverted to the packet filter, wherein the associated rule set is applied to validate the packet.

Therefore, unlike the claimed invention, there are no steps in either Shwed reference that, upon receipt of a packet to be validated, first selects a security policy from among a plurality of security policies and then applies the rules associated with that particular policy. Shwed merely applies a rule from the single rule set associated with the packet filter residing on that computer. In fact, Shwed '726 clearly states at column 2, lines 1-4, that a computer merely applies a given security policy to a packet and does not select a security policy from among a plurality of security policies, as in the claimed invention. That is, column 2, lines 1-4, of Shwed '726 states:

Another object of the invention is to provide a generic packet filter module which is controlled by a set of instructions to implement a given security policy at a node to accept (pass) or reject (drop) the packet wherein the packet is passed only if its passage is preauthorized. (Underlining added for emphasis).

Again, while a network administrator using the Shwed system may take into account different departments and individuals with varying titles at an organization, there is no escaping the fact that a packet filter protecting one or more than one computer is going to apply only the given security

policy embodied by the set of instructions programmed into the filter at the packet filter generator. There is no ability disclosed in the Shwed system to have a packet filter receive a packet, then select a security policy from among a plurality of security policies, and then apply the rule set associated with the selected policy. This is what the claimed invention is able to do, but not something that either Shwed reference can do.

For at least the above reasons, Applicants respectfully assert that independent claims 1, 8, 12, 17 and 22, and the claims which respectively depend therefrom, are patentable over both Shwed '726 and Shwed '668.

Further, regarding independent claim 16, both Shwed references fail to teach or suggest the elements of claim 16 including a domain comprising at least one security policy and a security policy comprising multiple rules, and that a plurality of administrators are associated with the plurality of domains, wherein multiple rules are administered such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain.

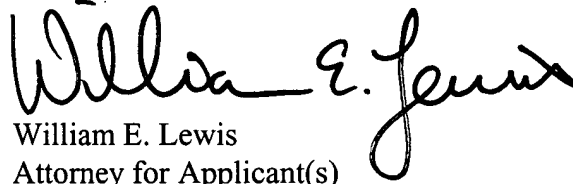
Assuming, *arguendo*, that the Office Action's assertion on page 6 is accurate (which Applicants' do not believe that it is) and that Shwed discloses multiple administrators, no where does either Shwed reference teach or suggest that, among a plurality of administrators associated with a plurality of domains, only an administrator for a given domain is permitted to modify rules of a security policy for that domain, as in claim 16.

For at least the above reasons, Applicants respectfully assert that independent claim 16 is patentable over both Shwed '726 and Shwed '668.

Accordingly, withdrawal of the §102(e) and §103(a) rejections of claims 1-26 is respectfully requested.

Applicants invite the Examiner to contact Applicants' attorney to discuss the above remarks and/or to resolve any remaining questions or issues.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "William E. Lewis". The signature is fluid and cursive, with a large, stylized "W" and "L".

Date: September 3, 2004

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan & Mason, L.L.P.
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946